

CLAIMS

We claim:

- 5           1.     A method for providing access to resources, comprising the steps of:  
              acquiring user identification information from a first authentication system,  
              said user identification information is associated with a request to access a first  
              resource, said step of acquiring is performed by an authorization system, said  
              authorization system is separate from said first authentication system;  
10           using said user identification information to access an identity profile  
              associated with said user identification information; and  
              performing authorization services for said request to access said first resource  
              based on said identity profile associated with said user identification information.
- 15           2.     A method according to claim 1, wherein:  
              said step of acquiring user identification includes reading a user ID from an  
              internal web server variable.
3.     A method according to claim 2, further comprising the step of:  
20           allowing a first user to access said first resource if said step of performing  
              determines that said first user is authorized to access said first resource based on said  
              identity profile, said first user is associated with said identity profile and said request.
4.     A method according to claim 1, further comprising the steps of:  
25           receiving information about said request;  
              determining whether said first resource is protected; and  
              determining that authentication for said first resource is to be performed by  
              said first authentication system.
- 30           5.     A method according to claim 1, wherein:

said step of acquiring user identification includes acquiring a plurality of data items which can be used to identify a user.

5           6.     A method according to claim 1, further comprising the step of:  
acquiring one or more data items in addition to said user identification  
information, said step of performing authorization services uses said one or more  
data items to attempt to authorize access to said first resource in response to said  
request.

10           7.     A method according to claim 1, wherein:  
said authorization system is part of an access system that protects a plurality  
of resources, said plurality of resources includes said first resource, a second  
resource and a third resource;  
said first resource uses said first authentication system for authentication  
15 services;  
said second resource uses a second authentication system for authentication  
services, said second authentication system is separate from said access system; and  
said third resource uses a third authentication system for authentication  
services, said third authentication system is separate from said access system.

20           8.     A method according to claim 7, wherein:  
said first authentication system is a default web server authentication system;  
said second authentication system is an authentication plug-in; and  
said third authentication system is a third party authentication system.

25           9.     A method according to claim 1, wherein:  
said authorization system is part of an access system that protects a plurality  
of resources, said access system provides for use of one or more internal  
authentication systems and said access system provides for reliance on one or more

external authentication systems, said one or more external authentication systems include said first authentication system.

10        10.     A method according to claim 1, wherein:  
5        said authorization system is part of an access system that protects a plurality of resources and does not have an application program interface.

11.     A method according to claim 1, further comprising the steps of:  
10        using said user identification information to create information for a cookie;  
and  
causing said cookie to be transmitted for storage on a client associated with said request.

12.     A method according to claim 11, further comprising the step of:  
15        performing single sign-on services based on said cookie.

13.     A method according to claim 11, further comprising the steps of:  
receiving a request to access a second resource, said request to access said  
second resource includes contents of said cookie; and  
20        using said cookie to authorize access to said second resource without  
authenticating.

14.     A method according to claim 11, further comprising the steps of:  
receiving a request to access a second resource at a second server, said  
25        request to access said first resource was received at a first server but not at said  
second server, said first authentication system does include said first server and does  
not include said second server, said step of receiving said request to access said  
second resource includes receiving contents of said cookie; and  
30        using said cookie at said second server to authorize access to said second  
resource without authenticating.

15. A method for providing access to resources, comprising the steps of:  
acquiring a plurality of variables from a first authentication system, said step  
of acquiring is performed by an authorization system, said authorization system is  
5 separate from said first authentication system, said variables are associated with a  
first request to access a first resource; and  
performing authorization services for said request to access said first resource  
based on said plurality of variables.

10 16. A method according to claim 15, further comprising the steps of:  
receiving information from said first request;  
determining whether said first resource is protected; and  
determining that authentication for said first resource is to be performed by  
said first authentication system.

15 17. A method according to claim 15, wherein:  
said authorization system is part of an access system that protects a plurality  
of resources, said access system provides for use of one or more internal  
authentication systems and said access system provides for reliance on one or more  
20 external authentication systems, said one or more external authentication systems  
include said first authentication system.

18. A method according to claim 15, further comprising the steps of:  
using said plurality of variables to create information for a cookie; and  
25 causing said cookie to be transmitted for storage on a client associated with  
said request.

19. A method according to claim 18, further comprising the step of:  
performing single sign-on services based on said cookie.

30

20. A method according to claim 18, further comprising the steps of:

receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does  
5 not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

10 21. A method for providing access to resources, comprising the steps of:

acquiring user identification information from an authentication system, said user identification information is associated with a request to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said authentication system;

15 using said user identification information to create information for a cookie;

causing said cookie to be transmitted for storage on a client associated with said request to access said first resource; and

performing authorization services for said request to access said first resource.

20 22. A method according to claim 21, wherein:

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more  
25 external authentication systems, said one or more external authentication systems include said first authentication system.

23. A method according to claim 21, further comprising the step of:

performing single sign-on services based on said cookie.

24. A method according to claim 21, further comprising the steps of:  
receiving a request to access a second resource, said request to access said  
second resource includes contents of said cookie; and  
using said cookie to authorize access to said second resource without  
5 authenticating.

25. A method according to claim 21, further comprising the steps of:  
receiving a request to access a second resource at a second server, said  
request to access said first resource was received at a first server but not at said  
10 second server, said first authentication system does include said first server and does  
not include said second server, said step of receiving said request to access said  
second resource includes receiving contents of said cookie; and  
using said cookie at said second server to authorize access to said second  
resource without authenticating.

26. A method for providing access to resources, comprising the steps of:  
receiving, at an access system, configuration information for a first resource,  
said access system provides for using of one or more internal authentication systems  
and said access system provides for reliance on one or more external authentication  
20 systems, said configuration information provides an indication to said access system  
to rely on a first external authentication system for said first resource;  
receiving a first request from a first user for said first resource;  
relying on said first external authentication system for authenticating said  
first user; and  
25 performing authorization services for said first request.

27. A method according to claim 26, wherein said one or more external  
authentication systems include:  
a default web server authentication system;  
30 an authentication plug-in; and

a third party authentication system.

28. A method according to claim 26, wherein:

5 said access system protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

said first resource uses said first authentication system for authentication services;

said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system; and

10 said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system.

29. A method according to claim 28, wherein:

15 said first authentication system is a default web server authentication system;

said second authentication system is a authentication plug-in; and

said third authentication system is a third party authentication system.

30. A method according to claim 26, wherein said step of relying includes:

20 accessing a pre-designated variable having a value; and

storing said value as an identification of an authenticated user.

31. A method according to claim 30, wherein said step of performing authorization services includes the steps of:

25 accessing one or more authorization rules for said first resource;

using said identification to access an identity profile; and

evaluating one or more attributes from said identity profile against said one or more authorization rules for said first resource to determine whether to authorize access to said first resource.

30

32. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

5 acquiring user identification information from a first authentication system, said user identification information is associated with a request to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said first authentication system;

10 using said user identification information to access an identity profile associated with said user identification information; and

performing authorization services for said request to access said first resource based on said identity profile associated with said user identification information.

33. One or more processor readable storage devices according to claim 15 32, wherein said method further comprises the steps of:

receiving information about said request;

determining whether said first resource is protected; and

determining that authentication for said first resource is to be performed by said first authentication system.

20 34. One or more processor readable storage devices according to claim 32, wherein said method further comprises the steps of:

25 acquiring one or more data items in addition to said user identification information, said step of performing authorization services uses said one or more data items to attempt to authorize access to said first resource in response to said request.

35. One or more processor readable storage devices according to claim 32, wherein:



03060515.106102

said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

36. One or more processor readable storage devices according to claim 32, wherein said method further comprises the steps of:  
using said user identification information to create information for a cookie;  
10 causing said cookie to be transmitted for storage on a client associated with said request; and  
performing single sign-on services based on said cookie.

37. One or more processor readable storage devices according to claim 15 32, wherein said method further comprises the steps of:  
using said user identification information to create information for a cookie;  
causing said cookie to be transmitted for storage on a client associated with said request;  
receiving a request to access a second resource at a second server, said  
20 request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and  
using said cookie at said second server to authorize access to said second  
25 resource without authenticating.

38. An access system, comprising:  
a communication interface;  
one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

5 acquiring user identification information from a first authentication system external to said access system, said user identification information is associated with a request to access a first resource,

using said user identification information to access an identity profile associated with said user identification information, and

10 performing authorization services for said request to access said first resource based on said identity profile associated with said user identification information.

39. An access system according to claim 38, wherein:

15 said access system protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

40. An access system according to claim 38, wherein said method further  
20 comprises the steps of:

using said user identification information to create information for a cookie;  
causing said cookie to be transmitted for storage on a client associated with said request;

25 receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

41. An access system according to claim 38, wherein said method further  
30 comprises the steps of:

receiving information about said request;  
determining whether said first resource is protected; and  
determining that authentication for said first resource is to be performed by  
said first authentication system.

5

42. One or more processor readable storage devices having processor  
readable code embodied on said processor readable storage devices, said processor  
readable code for programming one or more processors to perform a method  
comprising the steps of:

- 10 acquiring a plurality of variables from a first authentication system, said step  
of acquiring is performed by an authorization system, said authorization system is  
separate from said first authentication system, said variables are associated with a  
first request to access a first resource; and  
performing authorization services for said request to access said first resource  
15 based on said plurality of variables.

43. One or more processor readable storage devices according to claim  
42, wherein said method further comprises the steps of:  
receiving information from said first request;  
20 determining whether said first resource is protected; and  
determining that authentication for said first resource is to be performed by  
said first authentication system.

44. One or more processor readable storage devices according to claim  
25 42, wherein:  
said authorization system is part of an access system that protects a plurality  
of resources, said access system provides for use of one or more internal  
authentication systems and said access system provides for reliance on one or more  
external authentication systems, said one or more external authentication systems  
30 include said first authentication system.

45. One or more processor readable storage devices according to claim 42, wherein said method further comprises the steps of:

- using said plurality of variables to create information for a cookie;
- 5 causing said cookie to be transmitted for storage on a client associated with said request;
- receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and
- using said cookie to authorize access to said second resource without
- 10 authenticating.

46. An access system, comprising:
- a communication interface;
  - one or more storage devices; and
  - 15 one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

- acquiring a plurality of variables from a first authentication system external to said access system, said variables are associated with a first request to
- 20 access a first resource, and
- performing authorization services for said request to access said first resource based on said plurality of variables.

47. An access system according to claim 46, wherein said method further
- 25 comprises the steps of:
  - receiving information from said first request;
  - determining whether said first resource is protected; and
  - determining that authentication for said first resource is to be performed by said first authentication system.

30

48. An access system according to claim 46, wherein:

said access system protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

49. An access system according to claim 46, wherein said method further comprises the steps of:

using said plurality of variables to create information for a cookie;  
causing said cookie to be transmitted for storage on a client associated with said request;  
receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and  
using said cookie to authorize access to said second resource without authenticating.

50. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

acquiring user identification information from an authentication system, said user identification information is associated with a request to access a first resource, said step of acquiring is performed by an authorization system, said authorization system is separate from said authentication system;  
using said user identification information to create information for a cookie;  
causing said cookie to be transmitted for storage on a client associated with said request to access said first resource; and  
performing authorization services for said request to access said first resource.

51. One or more processor readable storage devices according to claim 50, wherein:

5 said authorization system is part of an access system that protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

52. One or more processor readable storage devices according to claim 10 50, wherein said method further comprises the step of:  
performing single sign-on services based on said cookie.

53. One or more processor readable storage devices according to claim 50, wherein said method further comprises the step of:  
15 receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and  
using said cookie to authorize access to said second resource without authenticating.

20 54. One or more processor readable storage devices according to claim 50, wherein said method further comprises the step of:  
receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does  
25 not include said second server, said step of receiving said request to access said second resource includes receiving contents of said cookie; and  
using said cookie at said second server to authorize access to said second resource without authenticating.

30 55. An access system, comprising:

a communication interface;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed

5 to perform a method comprising the steps of:

acquiring user identification information from an authentication system separate from said access system, said user identification information is associated with a request to access a first resource,

10 using said user identification information to create information for a cookie,

causing said cookie to be transmitted for storage on a client associated with said request to access said first resource, and

performing authorization services for said request to access said first resource.

15

56. An access system according to claim 55, wherein:

said access system protects a plurality of resources, said access system provides for use of one or more internal authentication systems and said access system provides for reliance on one or more external authentication systems, said one or more external authentication systems include said first authentication system.

20

57. An access system according to claim 55, wherein said method further comprises the step of:

performing single sign-on services based on said cookie.

25

58. An access system according to claim 55, wherein said method further comprises the step of:

receiving a request to access a second resource, said request to access said second resource includes contents of said cookie; and

using said cookie to authorize access to said second resource without authenticating.

5 59. An access system according to claim 55, wherein said method further comprises the step of:

receiving a request to access a second resource at a second server, said request to access said first resource was received at a first server but not at said second server, said first authentication system does include said first server and does not include said second server, said step of receiving said request to access said  
10 second resource includes receiving contents of said cookie; and

using said cookie at said second server to authorize access to said second resource without authenticating.

60. One or more processor readable storage devices having processor  
15 readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving, at an access system, configuration information for a first resource, said access system provides for using of one or more internal authentication systems  
20 and said access system provides for reliance on one or more external authentication systems, said configuration information provides an indication to said access system to rely on a first external authentication system for said first resource;

receiving information for a first request from a first user for said first resource;

25 relying on said first external authentication system for authenticating said first user; and

performing authorization services for said first request.



61. One or more processor readable storage devices according to claim 60, wherein:

said access system protects a plurality of resources, said plurality of resources includes said first resource, a second resource and a third resource;

5       said first resource uses said first authentication system for authentication services;

said second resource uses a second authentication system for authentication services, said second authentication system is separate from said access system;

10       said third resource uses a third authentication system for authentication services, said third authentication system is separate from said access system;

said first authentication system is a default web server authentication system;

said second authentication system is a authentication plug-in; and

said third authentication system is a third party authentication system.

15       62. One or more processor readable storage devices according to claim 60, wherein:

said step of relying includes accessing a pre-designated variable having a value and storing said value as an identification of an authenticated user; and

said step of performing authorization services includes the steps of:

20       accessing one or more authorization rules for said first resource,

using said identification to access an identity profile, and

evaluating one or more attributes from said identity profile against said one or more authorization rules for said first resource to determine whether to authorize access to said first resource.

25

63. An access system, comprising:

a communication interface;

one or more storage devices; and

one or more processors in communication with said one or more storage devices and said communication interface, said one or more processors programmed to perform a method comprising the steps of:

- 5 providing for using of one or more internal authentication systems,  
providing for reliance on one or more external authentication systems,  
receiving configuration information for a first resource, said  
configuration information provides an indication to rely on a first external  
authentication system for a first resource,  
receiving information for a first request from a first user for said first  
10 resource,  
relying on said first external authentication system for authenticating  
said first user, and  
performing authorization services for said first request.

- 15 64. An access system according to claim 63, wherein:  
said access system protects a plurality of resources, said plurality of resources  
includes said first resource, a second resource and a third resource;  
said first resource uses said first authentication system for authentication  
services;  
20 said second resource uses a second authentication system for authentication  
services, said second authentication system is separate from said access system;  
said third resource uses a third authentication system for authentication  
services, said third authentication system is separate from said access system;  
said first authentication system is a default web server authentication system;  
25 said second authentication system is a authentication plug-in; and  
said third authentication system is a third party authentication system.

65. An access system according to claim 63, wherein:  
said step of relying includes accessing a pre-designated variable having a  
30 value and storing said value as an identification of an authenticated user; and

- said step of performing authorization services includes the steps of:
- accessing one or more authorization rules for said first resource,
  - using said identification to access an identity profile, and
  - evaluating one or more attributes from said identity profile against said one or more
- 5 authorization rules for said first resource to determine whether to authorize access to said first resource.

09866515-062101